Tweede Kamer der Staten-Generaal 2

Vergaderjaar 2014–2015 Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1839

Vragen van het lid **Kooiman** (SP) aan de Minister van Veiligheid en Justitie over *het bericht dat de data van agenten niet goed beveiligd zijn* (ingezonden 26 februari 2015).

Antwoord van Minister **Van der Steur** (Veiligheid en Justitie) (ontvangen 7 april 2015). Zie ook Aanhangsel Handelingen, vergaderjaar 2014–2015, nr. 1722

Vraag 1, 2, 3 en 6
Hoe reageert u op het bericht dat de data van agenten niet goed beveiligd zijn?[1] [2]
Deelt u de mening dat de veiligheid van politiemensen in het geding kan komen wanneer gevoelige informatie over hen op straat komt te liggen?
Deelt u voorts de mening dat deze informatie daarom maximaal beveiligd moet zijn?
Hoe rijmt u het dat er veel energie is gestoken in het afschermen van gegevens van leden werkzaam bij units als Arrestatieteams, Observatieteams en Team Criminele Inlichtingen terwijl onbeveiligd via het internet kan worden ingelogd op systemen met deze gegevens? Kunt u uw antwoord toelichten?
Kunt u de garantie afgeven dat gevoelige informatie over politiepersoneel niet via hacking openbaar kan worden gemaakt? Biedt een dubbele inlogcode daartoe voldoende veiligheid? Zo nee, wat gaat u doen om die veiligheid wel te garanderen?

Antwoord 1, 2, 3 en 6
Ik vind de veiligheid van politiemensen en van hun persoonlijke gegevens van groot belang.
Bij de invoering van dit systeem, heeft de politie een risicoanalyse uitgevoerd naar de beveiliging van de hierin verwerkte gegevens.
Recent is naar aanleiding van signalen, doch niet naar aanleiding van incidenten of geconstateerde tekortkomingen, een tweede risicoanalyse

[1] «Data van agenten onveilig», Dagblad van het Noorden 25 februari 2015, http://www.dvhn.nl/nieuws/groningen/data-van-agenten-onveilig-12282293.html\
[2] Politie neemt extra maatregel beveiliging Youforce, Nationale Politie 25 februari 2015, http://www.politie.nl/nieuws/2015/februari/25/politie-neemt-extra-maatregel-beveiliging-youforce.html

ah-tk-20142015-1839
ISSN 0921 - 7398
’s-Gravenhage 2015

uitgevoerd. Naar aanleiding hiervan is een *Two Factor Authentication* toegevoegd, hetgeen hacken sterk bemoeilijkt.
De beveiliging van de persoonsgegevens die worden verwerkt met dit systeem voldoet aan de beveiligingseisen zoals gesteld in de Wet bescherming persoonsgegevens (Wbp). Een honderd procent veiligheidsgarantie bestaat niet op het terrein van informatiebeveiliging. Wel kan ik u garanderen dat op basis van risicoanalyses maatregelen zijn getroffen om de persoonsgegevens van politiepersoneel optimaal te beveiligen tegen verlies of ongeoorloofde toegang.
Het klopt overigens niet dat onbeveiligd kan worden ingelogd. Tevens is op geen enkel moment sprake geweest van toegang door onbevoegden.

Vraag 4 en 5
Hoe beoordeelt u de keuze om YouForce en VerzuimXpert onder te brengen bij een extern bedrijf? Is het wat u betreft verstandig deze gevoelige informatie te delen met organisaties buiten de Nationale Politie?
Is het niet veiliger dit computersysteem voor personeelszaken onder te brengen op een sterk beveiligde server van de politie zelf? Kunt u uw antwoord toelichten?

Antwoord 4 en 5
Het is niet ongebruikelijk dat de verwerking van personeelsgegevens wordt uitbesteed. Hier is dat ook het geval. Deze uitbesteding verandert echter niets aan de eisen die op basis van de Wbp worden gesteld aan de beveiliging van deze gegevens. Conform de Wbp blijft de korpschef verantwoordelijk voor een adequate beveiliging van deze gegevens.
Ook bij deze uitbesteding zijn eisen gesteld aan het gewenste niveau van beveiliging. De partij aan wie deze opdracht is uitbesteed, opereert onder Nederlandse wetgeving en heeft alle nodige maatregelen getroffen ter bescherming van de gegevens. Voorts verwijs ik u naar mijn antwoord op bovenstaande vragen.